PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-335239
(43)Date of publication of application : 22.11.2002

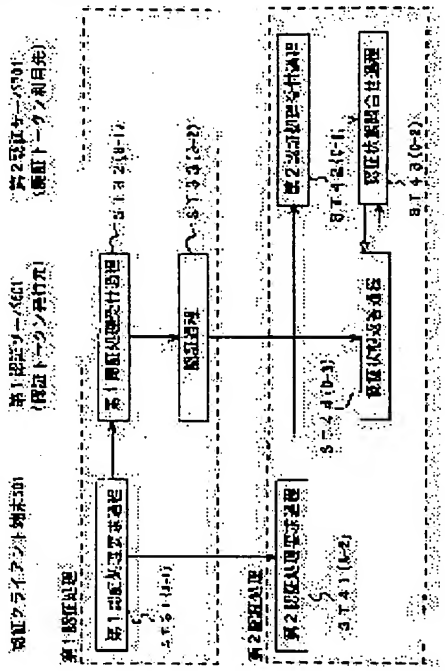
(51)Int.Cl. H04L 9/32
G06F 15/00
G09C 1/00
H04L 9/08

(21)Application number : 2001-138736
(22)Date of filing : 09.05.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : ITO KOJI
MORIMURA KAZUO

(54) METHOD AND SYSTEM DEVICE FOR AUTHENTICATING SINGLE SIGN- ON

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and system device for authenticating signal sign-on which enable reduction of a system construction cost and an operation managing cost by realizing a single sign-on function without requiring an authentication state managing server for unitarily managing an authentication state.
SOLUTION: This characteristic configuration method comprises first authentication processing where a first authentication server 601 to which a contents request (ST31) is applied from an authentication client terminal 501 operated by a user, performs (ST32) the authentication of the user, holds the authentication state as a result of the authentication performance and prepares/issues (ST33) an authentication token showing the authentication state and second authentication processing where a second authentication server 701 to which a contents request (ST41) is applied from the authentication client terminal 501 operated by the user and which accepts the request, performs processing (ST43) concerning the authentication of the user by utilizing (ST44) the authentication token prepared/issued in the first authenticating processing.



LEGAL STATUS

[Date of request for examination] 01.10.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－335239
（P2002－335239A）
(43)公開日　平成14年11月22日(2002.11.22)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
H04L 9/32		G06F 15/00	330B	5B085
G06F 15/00	330	G09C 1/00	640D	5J104
G09C 1/00	640	H04L 9/00	675D	
H04L 9/08			601C	

審査請求　未請求　請求項の数15　ＯＬ　（全 19 頁）

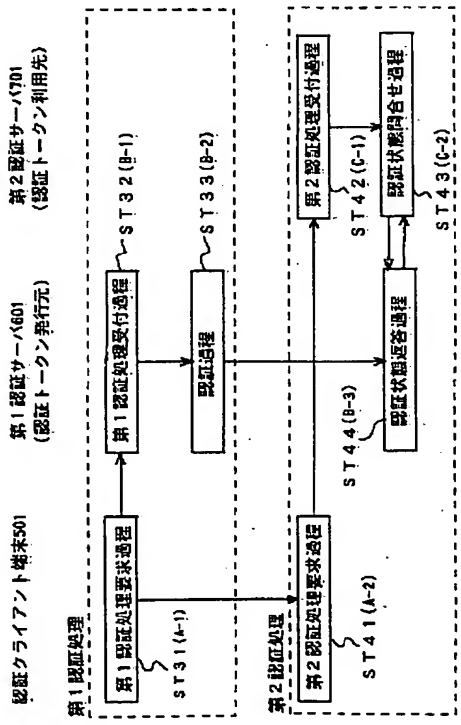
(21)出願番号　特願2001－138736(P2001－138736)
(22)出願日　平成13年５月９日(2001.5.9)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　伊藤　浩二
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　森村　一雄
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100071113
弁理士　菅　隆彦

最終頁に続く

(54)【発明の名称】　シングルサインオン認証方法及びシステム装置

(57)【要約】
【課題】認証状態を一元管理する認証状態管理サーバを必要とせずに、シングルサインオン機能を実現して、システム構築コスト及び運用管理コストを軽減することを可能とするシングルサインオン認証方法及びシステム装置の提供。
【解決手段】ユーザが操作する認証クライアント端末５０１からコンテンツ要求（ＳＴ３１）された第１認証サーバ６０１が、当該ユーザの認証を実行（ＳＴ３２）して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成発行（ＳＴ３３）する第１認証処理と、ユーザが操作する認証クライアント端末５０１からコンテンツ要求（ＳＴ４１）され、受付た（ＳＴ４２）第２認証サーバ７０１が、第１認証処理で作成発行された認証トークンを利用（ＳＴ４４）して、当該ユーザの認証についての処理（ＳＴ４３）を行なう第２認証処理と、を実施してなる特徴的構成手法の採用。



1

【特許請求の範囲】

【請求項１】特定のユーザに限定したサービスの提供をするために認証をするシステムに供され、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証方法であって、

前記複数のサーバにおける個々のサーバがユーザの認証状態を分散管理する、

ことを特徴とするシングルサインオン認証方法。

【請求項２】特定のユーザに限定したサービスの提供をするために認証をするシステムに供され、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証方法であって、

ユーザが操作する認証クライアント端末からコンテンツの要求をされた第１認証サーバが、当該ユーザの認証を実行して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成する第１認証処理と、

ユーザが操作する認証クライアント端末からコンテンツの要求をされた第２認証サーバが、前記第１認証処理で作成された前記認証トークンを利用して、当該ユーザの認証についての処理を行なう第２認証処理と、を実施してなる、

ことを特徴とするシングルサインオン認証方法。

【請求項３】前記第１認証処理は、

前記認証クライアント端末が前記第１認証サーバに対してコンテンツを要求することに応じて、当該認証クライアント端末についてのユーザの認証処理を要求する第１認証処理要求過程と、

当該第１認証処理要求過程で生じた認証処理の要求を前記第１認証サーバが受け付ける第１認証処理受付過程と、

当該第１認証処理受付過程で受けつけられた認証処理の要求につき、認証を実行して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成して、前記認証クライアント端末に発行する認証過程と、

を順次一貫経由して実施してなり、

前記第２認証処理は、

前記認証クライアント端末が前記第２認証サーバに対してコンテンツを要求することに応じて、当該認証クライアント端末についてのユーザの認証処理を要求する第２認証処理要求過程と、

当該第２認証処理要求過程で生じた認証処理の要求を前記第２認証サーバが受け付ける第２認証処理受付過程と、

当該第２認証処理受付過程で受けつけられた認証処理の要求につき、前記第１認証処理の認証過程で作成された前記認証トークンであって前記認証クライアント端末から送信された前記認証トークンに基づいて、前記第２認証サーバが、当該認証トークンの発行元である前記第１認証サーバに当該認証トークンの有効性を問合せる認証状態問合せ過程と、

当該認証状態問合せ過程で生じた前記認証トークンの有効性の問合せに対して、前記第１認証サーバが前記認証クライアント端末についてのユーザの認証状態を前記第２認証サーバに送信する認証状態返答過程と、

を順次一貫経由して実施してなる、

ことを特徴とする請求項２に記載のシングルサインオン認証方法。

【請求項４】前記認証過程は、

前記認証トークンを発行するときに、当該認証トークンの発行元である前記第１認証サーバを特定するものとなる電子的な署名を、当該認証トークンに含ませる署名作成処理をも実施する、

ことを特徴とする請求項３に記載のシングルサインオン認証方法。

【請求項５】前記認証過程は、

前記第１認証サーバ及び前記第２認証サーバで共有する共通鍵を用いて、前記認証トークンを暗号化して、前記認証クライアント端末に発行する共通鍵暗号処理をも実施する、

ことを特徴とする請求項４に記載のシングルサインオン認証方法。

【請求項６】前記シングルサインオン認証方法は、

前記第１認証サーバ及び前記第２認証サーバのそれぞれが、認証に関する各サーバの信頼性を表すパラメータとなる認証レベルを保持しており、

前記第２認証処理は、

前記認証トークンを受け取ったときに、当該第１認証サーバの認証レベルと当該第２認証サーバの認証レベルとを比較して、当該比較の結果に基づいて前記認証状態を管理する認証トークン検査更新処理をも実施する、

ことを特徴とする請求項５に記載のシングルサインオン認証方法。

【請求項７】前記認証トークン検査更新処理は、

前記第１認証サーバの認証レベルよりも前記第２認証サーバの認証レベルの方が高い場合は、前記認証状態を当該第２認証サーバで管理すると共に、当該第１認証サーバで管理されていた前記認証状態を破棄させ、

前記第２認証サーバの認証レベルよりも前記第１認証サーバの認証レベルの方が高い場合は、前記認証状態をそのまま当該第１認証サーバで管理させる、処理からなる、

ことを特徴とする請求項６に記載のシングルサインオン認証方法。

【請求項８】前記認証トークン検査更新処理は、

前記認証トークンを前記共通鍵を用いて復号化する共通鍵復号処理と、

前記署名作成処理で前記認証トークンに含められた署名を検証する署名検証処理と、

前記認証トークンに含まれるユーザの認証ＩＤを検証する認証ＩＤ検証処理と、
前記認証トークンに含まれる情報であって前記認証クライアント端末を特定する情報を検証するクライアント情報検証処理と、
前記認証トークンに含まれる情報である当該認証トークンの有効期限を検証する有効期限検証処理と、を実施して、
前記認証トークンの有効性を判断する処理も併せ実施する、
ことを特徴とする請求項７に記載のシングルサインオン認証方法。

【請求項９】特定のユーザに限定したサービスの提供をするために認証をするものにして、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証システム装置であって、
コンテンツを要求する認証クライアント端末と、
当該認証クライアント端末からのコンテンツ要求に応じて認証を実行し、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを当該認証クライアント端末に発行する第１認証サーバと、
前記認証クライアント端末からのコンテンツ要求に応じて認証を実行するときに、当該認証クライアント端末から前記認証トークンを受け取り、当該認証トークンの発行元である前記第１認証サーバに当該認証トークンの有効性につき問合せる第２認証サーバと、を有する、
ことを特徴とするシングルサインオン認証システム装置。

【請求項１０】　前記第１認証サーバは、
前記認証トークンを発行するときに、当該認証トークンの発行元である当該第１認証サーバを特定するものとなる電子的な署名を、当該認証トークンに付する署名作成部を有する、
ことを特徴とする請求項９に記載のシングルサインオン認証システム装置。

【請求項１１】前記第１認証サーバは、
当該第１認証サーバ及び前記第２認証サーバで共有する共通鍵を用いて、前記認証トークンを暗号化する共通鍵暗号部を有し、
当該共通鍵暗号部で暗号化された前記認証トークンを前記認証クライアント端末に発行自在な構成とする、
ことを特徴とする請求項１０に記載のシングルサインオン認証システム装置。

【請求項１２】前記第２認証サーバは、
前記認証トークンを受け取ったときに、前記第１認証サーバの認証レベルと当該第２認証サーバの認証レベルとを比較して、
当該第１認証サーバの認証レベルよりも当該第２認証サーバの認証レベルの方が高い場合は、前記認証状態を当該第２認証サーバで管理すると共に、当該第１認証サーバで管理されていた前記認証状態を破棄自在な構成とする、
ことを特徴とする請求項９、１０又は１１に記載のシングルサインオン認証システム装置。

【請求項１３】前記第１認証サーバ及び前記第２認証サーバは、
それぞれ、前記認証トークンの発行先を限定する信頼されるサーバリストを有し、
当該信頼されるサーバリストに挙げられているサーバに対してのみ、前記認証トークンを発行自在な構成とする、
ことを特徴とする請求項１２に記載のシングルサインオン認証システム装置。

【請求項１４】前記第１認証サーバ及び前記第２認証サーバは、
それぞれ、受け取った前記認証トークンの信頼判断に用いる信頼するサーバリストを有し、
受け取った前記認証トークンが当該信頼するサーバリストに挙げられているサーバが発行したものであるか確認自在な構成とする、
ことを特徴とする請求項１３に記載のシングルサインオン認証システム装置。

【請求項１５】前記第１認証サーバ及び前記第２認証サーバは、
それぞれ、
認証対象のユーザのＩＤと、当該ユーザのパスワードと、当該ユーザを特定する情報とを、相互に関連付けて保持する認証データベースと、
認証済みのユーザのＩＤと、当該ユーザのアクセスごとに変更される一時的なＩＤと、当該ユーザに操作される前記認証クライアント端末のアドレスと、当該ユーザの認証状態の有効期限と、当該ユーザを特定する情報とを、相互に関連付けて保持する認証状態管理データベースと、
を有してなる、
ことを特徴とする請求項１４に記載のシングルサインオン認証システム装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットを始めとするネットワーク上に存在する複数のサーバ（サーバ）において、ユーザの認証状態を共有し、特定のユーザに限定してサービスを提供するシステムに好適なものに関し、特に、認証状態を集中して管理するサーバを必要とせずに、複数の認証サーバで作成された認証状態を分散管理して相互に共通利用することを可能とするシングルサインオン認証方法及びシステム装置に関するものである。

【０００２】即ち、本発明は、ネットワーク上に存在する複数のサーバが認証状態を共用するシステムに好適な

シングルサインオン認証方法及びシステム装置に関するものである。ここで、認証状態とは、ユーザが既に認証済みであるか否かについての状態をいう。

【０００３】

【従来の技術】従来、ユーザが１回のログインで、複数のサーバにアクセスできるようにするシングルサインオン（single signon）という機能が考え出されている。複数のサーバが個々に認証を行なうと、ユーザはさまざまなユーザＩＤとパスワードを使い分ける必要が生じる。

【０００４】また管理という観点からも、複数パスワードを定期的に更新する手間を考えると、好ましくない。こうした環境において、ユーザの利便性と管理機能を向上させるため、ディレクトリサービスと同期して、複数サーバの認証とユーザのアクセス制御を一元管理するのがシングルサインオンとよばれる機能である。

【０００５】また、従来、ネットワーク上に存在する複数のサーバにおいて、シングルサインオンを用いて認証状態を共有し、特定のユーザに限定したサービスを提供するためには、認証状態を集中管理する認証状態管理サーバを設けていた。そして、各認証サーバが、ユーザの認証をする際に、認証状態管理サーバにユーザの認証状態を問合せることで、複数のサーバ間で認証状態を共有していた。

【０００６】図１２は、従来のシングルサインオン機能を持ったシステム装置の模式概念図である。同図において、認証クライアント端末１０１は、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistants）などからなる端末であり、処理プログラム１０２を内蔵している。

【０００７】インターネット又はイントラネット上には、認証クライアント端末１０１の他に、複数の認証サーバ２０１，３０１が存在し、その認証サーバ２０１，３０１はそれぞれ処理プログラム２０２，３０２を内蔵している。また、認証サーバ２０１，３０１は、それぞれ、認証処理が終了した後にクライアントに提供するコンテンツ２０３，３０３を持っている。

【０００８】更に、インターネット又はイントラネット上には、各認証サーバ２０１，３０１からの要求に応じて実際に認証処理及び認証状態の保持をする認証状態管理サーバ４０１が存在する。認証状態管理サーバ４０１は、処理プログラム４０２と、ＩＤ又はパスワードなどのユーザを認証するための情報を格納する認証データベース４０３と、ユーザの認証状態を保持する認証状態管理データベース４０４を持っている。

【０００９】図１３は、図１２に示す従来のシステム装置の処理手順を示すフローチャートである。ここでは、ユーザが認証クライアント端末１０１によって認証サーバ２０１（認証状態発行元）にアクセスして認証手続きを行なった後、認証サーバ３０１（認証状態利用先）にアクセスする場合を仮定する。

【００１０】先ず、認証処理要求過程ＳＴ１１（Ａ－１）からの認証要求は、認証処理受付過程ＳＴ１２（Ｂ－１）で受け付けられた後、認証過程ＳＴ１３（Ｄ－１）において認証処理及び認証状態の格納が行われる。その後、再び他の認証サーバ３０１に対して認証処理要求過程ＳＴ２１（Ａ－２）からの認証要求が発生した場合は、認証処理受付過程ＳＴ２２（Ｃ－１）で受け付けられた後、認証過程ＳＴ２３（Ｄ－２）において認証処理及び認証状態の格納が行われる。

【００１１】このとき、認証過程ＳＴ１３（Ｄ－１）で作成した認証状態が既に存在する場合は、その認証状態の情報を利用して認証が行われ、ユーザが認証に関する処理を再び行う必要はない。これらのように、複数の認証サーバ２０１、３０１が認証を行う場合に、認証状態の管理を認証状態管理サーバ４０１が一括して行うことにより、認証状態を共有してシングルサインオンを実現している。

【００１２】

【発明が解決しようとする課題】上述のように、従来は、ネットワーク上に存在する複数のサーバ（認証サーバ２０１、３０１）において、認証状態を共有し、特定のユーザに限定したサービスを提供するために、認証状態を特設した専門の認証状態管理サーバ４０１において一元的に管理している。これにより、認証状態を確実に管理し、ユーザが認証に関わる作業を繰り返し行う必要がなくなるシングルサインオンが実現する。

【００１３】しかしながら、このような従来の手法では、認証状態管理サーバ４０１に処理が集中するために、認証状態管理サーバ４０１には特に高い処理能力が求められ、多額の運用資金と高度な運用スキルが求められる。このことにより小規模サイトにおいては、シングルサインオンとして運用することがコスト面及び運用面で困難なものとなっている。

【００１４】また、従来の手法では、ネットワーク上においてシングルサインオンを実現するときに、シングルサインオンを実施するサーバ群の認証状態の信頼性は常に均一となっているものではなく、各サーバ間で信頼性の高低が生ずる。また、ネットワーク上で認証状態を交換するときに、盗聴、改ざん、成りすまし等のネットワーク特有の危険性も存在している。

【００１５】ここにおいて、本発明の解決すべき主要な目的は以下の通りである。即ち、本発明の第１の目的は、ユーザが１回のログインで複数のサーバにアクセス可能となるシングルサインオン機能を持つシステムについて、認証状態を一元管理する認証状態管理サーバを必要とせずに、システム構築コスト及び運用管理コストを軽減することを可能とするシングルサインオン認証方法及びシステム装置を提供せんとするものである。

【００１６】本発明の第２の目的は、複数の認証サーバ

間において認証に関する信頼性につき優劣があっても、認証状態の適切な管理を可能とするシングルサインオン認証方法及びシステム装置を提供せんとするものである。

【００１７】本発明の第３の目的は、複数の認証サーバ（サーバ）間でネットワークを介して認証状態を相互に利用しても、セキュリティを確保することを可能とするシングルサインオン認証方法及びシステム装置を提供せんとするものである。

【００１８】本発明の他の目的は、明細書、図面、特に、特許請求の範囲における各請求項の記載から自ずと明らかとなろう。

【００１９】

【課題を解決するための手段】本発明装置は、上記課題の解決に当たり、ユーザが既に認証済みであるかの状態を示す認証状態を、選択分散管理する複数の認証サーバを有してなる構成手段を講じる特徴を有する。

【００２０】本発明方法は、上記課題の解決に当たり、認証サーバは、他の認証サーバによって認証された情報である認証トークンを認証クライアント端末から受け取った際に、認証トークン発行元の認証サーバに対する問合せ電文を作成して、受け取った認証トークンの有効性を検証する構成手法を講じる特徴を有する。

【００２１】更に、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念にわたる新規な特徴的構成手法又は手段を採用することにより、上記目的を達成するように為される。

【００２２】即ち、本発明方法の第１の特徴は、特定のユーザに限定したサービスの提供をするために認証をするシステムに供され、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証方法であって、前記複数のサーバにおける個々のサーバがユーザの認証状態を分散管理してなるシングルサインオン認証方法の構成採用にある。

【００２３】本発明方法の第２の特徴は、特定のユーザに限定したサービスの提供をするために認証をするシステムに供され、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証方法であって、ユーザが操作する認証クライアント端末からコンテンツの要求をされた第１認証サーバが、当該ユーザの認証を実行して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成する第１認証処理と、ユーザが操作する認証クライアント端末からコンテンツの要求をされた第２認証サーバが、前記第１認証処理で作成された前記認証トークンを利用して、当該ユーザの認証についての処理を行なう第２認証処理と、を実施してなるシングルサインオン認証方法の構成採用にある。

【００２４】本発明方法の第３の特徴は、上記本発明方法の第２の特徴における前記第１認証処理が、前記認証クライアント端末が前記第１認証サーバに対してコンテンツを要求することに応じて、当該認証クライアント端末についてのユーザの認証処理を要求する第１認証処理要求過程と、当該第１認証処理要求過程で生じた認証処理の要求を前記第１認証サーバが受け付ける第１認証処理受付過程と、当該第１認証処理受付過程で受けつけられた認証処理の要求につき、認証を実行して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成して、前記認証クライアント端末に発行する認証過程と、を順次一貫経由して実施してなり、前記第２認証処理は、前記認証クライアント端末が前記第２認証サーバに対してコンテンツを要求することに応じて、当該認証クライアント端末についてのユーザの認証処理を要求する第２認証処理要求過程と、当該第２認証処理要求過程で生じた認証処理の要求を前記第２認証サーバが受け付ける第２認証処理受付過程と、当該第２認証処理受付過程で受けつけられた認証処理の要求につき、前記第１認証処理の認証過程で作成された前記認証トークンであって前記認証クライアント端末から送信された前記認証トークンに基づいて、前記第２認証サーバが、当該認証トークンの発行元である前記第１認証サーバに当該認証トークンの有効性を問合せる認証状態問合せ過程と、当該認証状態問合せ過程で生じた前記認証トークンの有効性の問合せに対して、前記第１認証サーバが前記認証クライアント端末についてのユーザの認証状態を前記第２認証サーバに送信する認証状態返答過程と、を順次一貫経由して実施してなるシングルサインオン認証方法の構成採用にある。

【００２５】本発明方法の第４の特徴は、上記本発明方法の第３の特徴における前記認証過程が、前記認証トークンを発行するときに、当該認証トークンの発行元である前記第１認証サーバを特定するものとなる電子的な署名を、当該認証トークンに含ませる署名作成処理をも実施してなるシングルサインオン認証方法の構成採用にある。

【００２６】本発明方法の第５の特徴は、上記本発明方法の第４の特徴における前記認証過程が、前記第１認証サーバ及び前記第２認証サーバで共有する共通鍵を用いて、前記認証トークンを暗号化して、前記認証クライアント端末に発行する共通鍵暗号処理をも実施してなるシングルサインオン認証方法の構成採用にある。

【００２７】本発明方法の第６の特徴は、上記本発明方法の第５の特徴における前記シングルサインオン認証方法が、前記第１認証サーバ及び前記第２認証サーバのそれぞれが、認証に関する各サーバの信頼性を表すパラメータとなる認証レベルを保持しており、前記第２認証処理は、前記認証トークンを受け取ったときに、当該第１認証サーバの認証レベルと当該第２認証サーバの認証レベルとを比較して、当該比較の結果に基づいて前記認証状態を管理する認証トークン検査更新処理をも実施して

なるシングルサインオン認証方法の構成採用にある。

【００２８】本発明方法の第７の特徴は、上記本発明方法の第６の特徴における前記認証トークン検査更新処理が、前記第１認証サーバの認証レベルよりも前記第２認証サーバの認証レベルの方が高い場合は、前記認証状態を当該第２認証サーバで管理すると共に、当該第１認証サーバで管理されていた前記認証状態を破棄させ、前記第２認証サーバの認証レベルよりも前記第１認証サーバの認証レベルの方が高い場合は、前記認証状態をそのまま当該第１認証サーバで管理させる、処理からなるシングルサインオン認証方法の構成採用にある。

【００２９】本発明方法の第８の特徴は、上記本発明方法の第７の特徴における前記認証トークン検査更新処理が、前記認証トークンを前記共通鍵を用いて復号化する共通鍵復号処理と、前記署名作成処理で前記認証トークンに含められた署名を検証する署名検証処理と、前記認証トークンに含まれるユーザの認証ＩＤを検証する認証ＩＤ検証処理と、前記認証トークンに含まれる情報であって前記認証クライアント端末を特定する情報を検証するクライアント情報検証処理と、前記認証トークンに含まれる情報である当該認証トークンの有効期限を検証する有効期限検証処理と、を実施して、前記認証トークンの有効性を判断する処理も併せ実施してなるシングルサインオン認証方法の構成採用にある。

【００３０】本発明装置の第１の特徴は、特定のユーザに限定したサービスの提供をするために認証をするものにして、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証システム装置であって、コンテンツを要求する認証クライアント端末と、当該認証クライアント端末からのコンテンツ要求に応じて認証を実行し、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを当該認証クライアント端末に発行する第１認証サーバと、前記認証クライアント端末からのコンテンツ要求に応じて認証を実行するときに、当該認証クライアント端末から前記認証トークンを受け取り、当該認証トークンの発行元である前記第１認証サーバに当該認証トークンの有効性につき問合せる第２認証サーバと、を有してなるシングルサインオン認証システム装置の構成採用にある。

【００３１】本発明装置の第２の特徴は、上記本発明装置の第１の特徴における前記第１認証サーバが、前記認証トークンを発行するときに、当該認証トークンの発行元である当該第１認証サーバを特定するものとなる電子的な署名を、当該認証トークンに付する署名作成部を有してなるシングルサインオン認証システム装置の構成採用にある。

【００３２】本発明装置の第３の特徴は、上記本発明装置の第２の特徴における前記第１認証サーバが、当該第１認証サーバ及び前記第２認証サーバで共有する共通鍵を用いて、前記認証トークンを暗号化する共通鍵暗号部を有し、当該共通鍵暗号部で暗号化された前記認証トークンを前記認証クライアント端末に発行自在な構成としてなるシングルサインオン認証システム装置の構成採用にある。

【００３３】本発明装置の第４の特徴は、上記本発明装置の第１、第２又は第３の特徴における前記第２認証サーバが、前記認証トークンを受け取ったときに、前記第１認証サーバの認証レベルと当該第２認証サーバの認証レベルとを比較して、当該第１認証サーバの認証レベルよりも当該第２認証サーバの認証レベルの方が高い場合は、前記認証状態を当該第２認証サーバで管理すると共に、当該第１認証サーバで管理されていた前記認証状態を破棄自在な構成としてなるシングルサインオン認証システム装置の構成採用にある。

【００３４】本発明装置の第５の特徴は、上記本発明装置の第４の特徴における前記第１認証サーバ及び前記第２認証サーバが、それぞれ、前記認証トークンの発行先を限定する信頼されるサーバリストを有し、当該信頼されるサーバリストに挙げられているサーバに対してのみ、前記認証トークンを発行自在な構成としてなるシングルサインオン認証システム装置の構成採用にある。

【００３５】本発明装置の第６の特徴は、上記本発明装置の第５の特徴における前記第１認証サーバ及び前記第２認証サーバが、それぞれ、受け取った前記認証トークンの信頼判断に用いる信頼するサーバリストを有し、受け取った前記認証トークンが当該信頼するサーバリストに挙げられているサーバが発行したものであるか確認自在な構成としてなるシングルサインオン認証システム装置の構成採用にある。

【００３６】本発明装置の第７の特徴は、上記本発明装置の第６の特徴における前記第１認証サーバ及び前記第２認証サーバが、それぞれ、認証対象のユーザのＩＤと、当該ユーザのパスワードと、当該ユーザを特定する情報とを、相互に関連付けて保持する認証データベースと、認証済みのユーザのＩＤと、当該ユーザのアクセスごとに変更される一時的なＩＤと、当該ユーザに操作される前記認証クライアント端末のアドレスと、当該ユーザの認証状態の有効期限と、当該ユーザを特定する情報とを、相互に関連付けて保持する認証状態管理データベースと、を有してなるシングルサインオン認証システム装置の構成採用にある。

【００３７】これらにより、本発明は、従来認証状態管理サーバが一元管理していた認証状態を、個々の認証サーバが相互に認証レベルを比較して選択分散管理するので、従来必要とされた認証状態管理サーバの運用・構築コストを削減することができる。即ち、個々の認証サーバは、他の認証サーバによって認証された情報（認証トークン）を認証クライアント端末から受け取った際に、認証トークン発行元の認証サーバに対する問合せ電文を

作成し、受け取った認証トークンの有効性を検証する。

【００３８】また、本発明の選択分散管理は、複数の認証サーバ間における認証に関する信頼性の優劣を意識した認証状態の適切な管理を行うために、それぞれの認証サーバ（サーバ）に認証に関する信頼性を表すパラメータ（認証レベル）を付与する。そして、認証トークン発行元の認証サーバに認証トークンの有効性を確認する際に、認証トークン発行元の認証サーバの認証レベルが認証トークン利用先の認証サーバの認証レベルを上回る場合は、認証状態はそのまま認証トークン発行元の認証サーバで管理される。

【００３９】一方、認証トークン発行元の認証サーバの認証レベルが認証トークン利用先の認証レベルを下回る場合は、認証状態は新たに認証トークン利用先において管理されると共に、認証トークン発行元の認証サーバで管理されていた情報（認証状態）は破棄される。このような手段を用いることにより、本発明によれば、各認証サーバ（サーバ）間に認証レベルの優劣が存在する場合における認証状態の適切な管理が可能となる。

【００４０】更に、本発明は、各認証サーバ（サーバ）間の認証状態の相互利用におけるセキュリティ維持について、各認証サーバは相互に共通な共通鍵を持ち、問合せ電文及び応答電文の暗号化を行う。また、各認証サーバは、それぞれ「信頼するサーバの一覧」と「信頼されるサーバの一覧」を持ち、認証トークン発行時には信頼されるサーバに対して認証トークンを発行し、他のサーバが発行した認証トークンを利用する場合には信頼するサーバが発行した認証トークンであることを確認する。

【００４１】更にまた、本発明は、認証サーバ間でやり取りされる電文は各認証サーバの秘密鍵により電子的に署名され、認証状態の偽造・改ざん・なりすましを防止する。これらにより、本発明は、認証状態を選択分散管理して、安全、簡易且つ柔軟に認証状態を共有することを可能とする。

【００４２】

【発明の実施の形態】以下、添付図面を参照しながら、本発明の実施の形態を装置例及び方法例につき説明する。

【００４３】なお、本発明は、ネットワーク上において、ユーザの認証状態を複数のサーバが共有して、ユーザが１回のログインで複数のサーバにアクセスできるようにするシングルサインオンをなすものであって、認証状態を複数のサーバで選択分散管理するものであるが、本実施形態では、ネットワークとしてとして専らインターネット／イントラネットを代表例として説明するも、本発明はこれ等に限定されるものではない。

【００４４】（装置例）図１は、本発明の装置例に係るシングルサインオン認証システム装置の概念模式図である。図中、２はインターネット及びイントラネットなどからなるネットワーク、５０１はパーソナルコンピュータ又はＰＤＡなどからなる認証クライアント端末である。

【００４５】６０１は認証クライアント端末からのコンテンツ要求に応じて認証を実行する第１認証サーバ、７０１は認証クライアント端末からのコンテンツ要求に応じて認証を実行する第２認証サーバである。認証クライアント端末５０１、第１認証サーバ６０１及び第２認証サーバ７０１は、相互にネットワーク２を介して接続される。

【００４６】認証クライアント端末５０１は、第１認証サーバ６０１及び第２認証サーバ７０１に対してコンテンツを要求するものであり、自身の動作を規定する処理プログラム５０２を内蔵している。第１認証サーバ６０１は、自身の動作を規定する処理プログラム６０２を内蔵している。第２認証サーバ７０１は、自身の動作を規定する処理プログラム７０２を内蔵している。

【００４７】また、第１認証サーバ６０１は、認証したクライアント（認証クライアント端末５０１）に対して送信するＷＷＷコンテンツ６０３と、認証処理に用いるデータからなる認証データベース６０４と、認証状態の保持及び管理をする認証状態管理データベース６０５と、認証トークンの発行先を限定する「信頼されるサーバリスト」６０６と、受け取った認証トークンを信頼するか否かの判断に用いる信頼するサーバリスト６０７とを備えている。

【００４８】第２認証サーバ７０１も、第１認証サーバ６０１と同様に、認証したクライアント（認証クライアント端末５０１）に対して送信するＷＷＷコンテンツ７０３と、認証処理に用いるデータからなる認証データベース７０４と、認証状態の保持及び管理をする認証状態管理データベース７０５と、認証トークンの発行先を限定する「信頼されるサーバリスト」７０６と、受け取った認証トークンを信頼するか否かの判断に用いる「信頼するサーバリスト」７０７とを備えている。

【００４９】ここで、認証トークンとは、各クライアントの認証状態を示す情報からなるものであり、認証クライアント端末５０１からのコンテンツ要求に応じて、第１認証サーバ６０１（又は第２認証サーバ７０１）が認証する際に作成されるものであり、詳細は後述する。

【００５０】本実施形態では、第１認証サーバ６０１を認証トークン発行元として、第２認証サーバ７０１を認証トークン利用先としているが、これは説明上仮定したものである。即ち、第１認証サーバ６０１と第２認証サーバ７０１は、それぞれ同じ機能を持ち、それぞれ認証トークン発行元になり且つ認証トークン利用先ともなる。

【００５１】即ち、第１認証サーバ６０１は、認証クライアント端末５０１からのコンテンツ要求に応じて認証を実行し、当該認証実行の結果である認証状態を認証状態管理データベース６０５で保持及び管理し、当該認証

状態を示す認証トークンを当該認証クライアント端末に発行するものである。

【００５２】第２認証サーバ７０１は、認証クライアント端末５０１からのコンテンツ要求に応じて認証を実行するときに、認証クライアント端末５０１から認証トークンを受け取り、その認証トークンの発行元である第１認証サーバ６０１に当該認証トークンの有効性につき問合せるものである。

【００５３】図２は、本装置例に係るシングルサインオン認証システム装置の動作を示すフローチャートである。本図では、第１認証処理として、ユーザが認証クライアント端末５０１から第１認証サーバ６０１（認証トークン発行元）にアクセスして認証手続きを行った後、第２認証処理として、第２認証サーバ７０１（認証トークン利用先）にアクセスする場合を仮定して、示している。

【００５４】先ず、認証クライアント端末５０１で実行される認証処理要求過程ＳＴ３１（Ａ－１）からの認証要求は、第１認証サーバ６０１の認証処理受付過程ＳＴ３２（Ｂ－１）で受け付けられた後、第１認証サーバ６０１の認証過程ＳＴ３３（Ｂ－２）で認証処理及び認証状態の格納が行われる。

【００５５】その後、再び認証クライアント端末５０１において、認証処理要求過程ＳＴ４１（Ａ－２）からの認証要求が他のサーバ（第２認証サーバ７０１）に対して発生した場合は、その認証要求が第２認証サーバ７０１の認証処理受付過程ＳＴ４２（Ｃ－１）で受け付けられる。

【００５６】ここで、他のサーバ（第１認証サーバ６０１）によって認証された認証トークンがその認証要求に添付されている場合には、第２認証サーバ７０１の認証状態問合せ過程ＳＴ４３（Ｃ－２）で、第１認証サーバ６０１の認証状態返答過程ＳＴ４４（Ｂ－３）に対しての認証状態についての問合せが実行される。

【００５７】そして、第２認証サーバ７０１の認証状態問合せ過程ＳＴ４３（Ｃ－２）において、認証トークンの有効性につき確認され、有効性が確認された場合はいずれのサーバ（第１認証サーバ６０１又は第２認証サーバ７０１）が認証状態を保持及び管理すべきかの判定が行われ、その判定に基づいて認証状態の保持及び管理が実行される。

【００５８】これらにより、第１認証処理における認証過程ＳＴ３３（Ｂ－１）で認証状態が作成されるので、第２認証処理においては認証過程ＳＴ３３（Ｂ－１）で作成された認証状態を利用して認証が行われ、ユーザが認証に関する処理を再び行う必要はない。

【００５９】図３は、第１認証サーバ６０１及び第２認証サーバ７０１がそれぞれ具備するデータベースの構造を示す図である。

【００６０】図中、（ａ）は認証データベース６０４，７０４の構造を示し、（ｂ）は認証状態管理データベース６０５，７０５の構造を示している。認証データベース６０４，７０４は、認証対象のユーザのＩＤであるユーザＩＤと、当該ユーザのパスワードと、当該ユーザを特定する情報などとを、相互に関連付けて保持するものである。

【００６１】認証状態管理データベース６０５，７０５は、認証済みのユーザのＩＤであるユーザＩＤと、当該ユーザのアクセスごとに変更される一時的なＩＤである認証ＩＤと、当該ユーザに操作される認証クライアント端末５０１のアドレスと、当該ユーザの認証状態の有効期限と、当該ユーザを特定する情報とを、相互に関連付けて保持するものである。

【００６２】次に、本実施形態の方法例として、あるユーザが第１認証サーバ６０１において認証をした後、

１）再び、同じサーバである第１認証サーバ６０１に対して認証をする場合、

２）異なるサーバである第２認証サーバ７０１に対して認証を行う場合であって、（第１認証サーバ601の認証レベル）≧（第２認証サーバ701の認証レベル）である場合、

３）異なるサーバである第２認証サーバ７０１に対して認証を行う場合であって、（第１認証サーバ601の認証レベル）＜（第２認証サーバ701の認証レベル）である場合、

の３通りの場合に分けて、説明する。

【００６３】ここで、認証レベルとは、各認証サーバに付されるものであって、認証に関する各認証サーバの信頼性を表すパラメータとなるものであり、認証レベルの高い認証サーバが管理する認証状態ほど、信頼性の高い認証がなされているものとする。

【００６４】そして、各認証サーバ（第１認証サーバ６０１及び第２認証サーバ７０１）は、認証トークンを利用して認証状態を共有するので、第２認証サーバ７０１に対する認証時には、ユーザは認証処理を改めて行う必要がない。即ち、シングルサインオンが実行される。

【００６５】（方法例１）前記装置例に適用する本実施形態例の方法例１につき図４乃至及び図８を参照して説明する。方法例１は、あるユーザが第１認証サーバ６０１において認証をした後、再び、同じサーバである第１認証サーバ６０１に対して認証をする場合に、適用される手法である。

【００６６】図４は、ユーザが認証サーバ群に初めて認証を求めるときの手順を示すフローチャートである。いま、ユーザが認証サーバ群（第１認証サーバ６０１及び第２認証サーバ７０１）に対して、初めて認証をすると仮定する。即ち、認証クライアント端末５０１が第１認証サーバ６０１又は第２認証サーバ７０１に対して、初めてコンテンツの要求をする場合である。このときの処理手順が図３に示されている。

15

【００６７】先ず、ユーザは、認証クライアント端末５０１の処理プログラム５０２を起動させて、その処理プログラム５０２に含まれているコンテンツ要求部５０３から第１認証サーバ６０１の処理プログラム６０２の認証開始部６０８に対して、コンテンツを要求する。

【００６８】認証開始部６０８は、コンテンツの要求を受けた後、その要求内容が認証を必要とするものか判断し、認証が必要である場合は認証処理部６０９を呼び出す。認証処理部６０９は、コンテンツの要求に「認証済みの認証トークン」が付属していないことを確認し、認証データベース６０４から認証に必要なデータを取得して、認証処理を行う。

【００６９】ここで、認証が正常に完了した場合は、認証処理部６０９はコンテンツ返却部６１０を呼び出す。コンテンツ返却部６１０では、WWWコンテンツ６０３から要求に係るコンテンツを取得し、「信頼されるサーバリスト」６０６から認証トークンの配布先を取得し、認証トークン作成部６１１で作成された認証トークンを取得したコンテンツに添付して、そのコンテンツを認証クライアント端末５０１に返却する。

【００７０】図５は、認証トークン作成部６１１における処理手順を示すフローチャートである。図６は、第１認証サーバ６０１及び第２認証サーバ７０１で作成される各種電文の構造を示す概念模式図である。ここで、図６（ａ）は、認証トークン作成部６１１で作成された認証トークンの構造を示す概念模式図である。なお、図６（ｂ）、（ｃ）、（ｄ）については後述する。

【００７１】先ず、認証トークン作成部６１１は、有効期限作成部６１２において指定された有効期限を作成する（有効期限作成処理）。その後、認証ＩＤ作成部６１３において乱数からなる認証ＩＤを作成する（認証ＩＤ作成処理）。その後、作成された有効期限、認証ＩＤ及び認証クライアント端末５０１を特定するクライアント情報を認証状態管理データベース６０５に登録する。

【００７２】その後、署名作成部６１４において認証トークンを作成した認証サーバ（第１認証サーバ６０１）の署名を作成する（署名作成処理）。その後、共通鍵暗号部６１５において、認証トークン全体を各認証サーバが共通に持つ共通鍵によって暗号化する（共通鍵暗号処理）。そして、暗号化された認証トークンは、コンテンツ返却部６１０に送られ、コンテンツと共に認証クライアント端末５０１に送信される。

【００７３】次に、ユーザが過去に認証を求めた第１認証サーバに対して、再び認証を求める場合について説明する。図７は、同一の認証サーバに再度の認証要求が発生した場合の処理手順を示すフローチャートである。

【００７４】先ず、認証クライアント端末５０１の処理プログラム５０２が起動され、その処理プログラム５０２に含まれるコンテンツ要求部５０３から第１認証サーバ６０１の処理プログラム６０２の認証開始部６０８に対して、コンテンツを要求する。

16

【００７５】その要求を受け取った認証開始部６０８は、その要求内容につき認証が必要か判断し、必要と判断した場合は認証処理部６０９を呼び出す。認証処理部６０９は、認証済みの認証トークンが、受け取ったコンテンツ要求に付属されていることを確認し、認証トークン検証／更新部６１６をよぶ。

【００７６】図８は、認証トークン検証／更新部６１６の処理手順を示すフローチャートである。認証トークン検証／更新部６１６では、先ず、認証トークン発行者検証部６１７が「信頼するサーバリスト６０７」を利用して、認証トークンの認証レベルを検証する。この方法例１では同一のサーバ（第１認証サーバ）が発行した認証トークンを同一のサーバ（第１認証サーバ）で利用するため、認証レベルの比較は不要となる。

【００７７】次に、共通鍵復号部６１８において認証トークンが共通鍵で復号化される（共通鍵復号処理）。引続き、署名検証部６１９において認証トークンに含まれる署名が検証される（署名検証処理）。その後、認証ＩＤ検証部６２０において前記認証トークンに含まれるユーザの認証ＩＤが検証される（認証ＩＤ検証処理）。

【００７８】そして、クライアント情報検証部６２１において、認証トークンに含まれる情報であって認証クライアント端末５０１を特定する情報が検証される（クライアント情報検証処理）。更に、有効期限検証部６２２において認証トークンに含まれる情報である当該認証トークンの有効期限が検証される（有効期限検証処理）。

【００７９】これらに処理により、信頼できるサーバから有効な認証トークンが得られたことが検証される。その後、有効期限更新部６２３において新たな有効期限が作成され、認証ＩＤ更新部６２４において新たな認証ＩＤが生成され、認証状態管理データベース６０５にその新たな有効期限及び認証ＩＤが登録される。その後、署名作成部６２５においてクライアント情報と共に署名が生成され、共通鍵暗号部６２６において新たな認証トークンの全体が共通鍵で暗号化される

【００８０】これらの処理の後、「信頼されるホストリスト６０６」を用いて認証トークンの配布先を特定し、コンテンツ返却部６１０は、WWWコンテンツ６０３から要求対象のコンテンツを取得して、新たな認証トークンと共に認証クライアント端末５０１に送付する。

【００８１】（方法例２）前記装置例に適用する本実施形態例の方法例２につき図６及び図９を参照して説明する。方法例２は、あるユーザが第１認証サーバ６０１において認証をした後、第１認証サーバ６０１とは異なるサーバである第２認証サーバ７０１に対して認証をする場合に、適用される手法である。

【００８２】そして、方法例２では、第１認証サーバ６０１（認証トークン発行元）の認証レベルが、第２認証サーバ７０１（認証トークン利用先）の認証レベル以上

であると、仮定する。先ず、前述の方法例１と同様に、ユーザが認証サーバ群（第1認証サーバ６０１及び第２認証サーバ７０１）に対して、初めて認証を行うとする。その後、第１認証サーバ６０１とは異なる第２認証サーバ７０１に対して、認証要求を行うとする。このときの処理手順が図９に示されている。

【００８３】図９は、認証トークン発行先の認証サーバの認証レベルが認証トークン利用先の認証サーバの認証レベル以上である場合の処理手順を示すフローチャートである。

【００８４】先ず、ユーザは、認証クライアント端末５０１の処理プログラム５０２を起動させて、その処理プログラム５０２に含まれているコンテンツ要求部５０３から第２認証サーバ７０１の処理プログラム７０２の認証開始部７０８に対して、第１認証サーバ６０１で作成された認証トークンを伴なったコンテンツ要求情報を送信することで、コンテンツを要求する。

【００８５】認証開始部７０８は、コンテンツ要求情報を受けた後、その要求内容が認証を必要とするものか判断し、認証が必要である場合は認証処理部７０９を呼び出す。認証処理部７０９は、コンテンツ要求情報に「認証済みの認証トークン」が付属していることを確認し、「信頼するサーバリスト７０７」を参照して、信頼するサーバによって作成された認証トークンであることを確認する。

【００８６】その後、問合せ電文作成部７２７は、図６（ｂ）に示す問合せ電文を作成し、認証トークン発行元の第１認証サーバ６０１の処理プログラム６０２の問合せ電文受付部６２９に暗号化された電文を送信する。

【００８７】図６（ｂ）は、問合せ電文作成部７２７で作成された問合せ電文の構造を示す概念模式図である。問合せ電文受付部６２９は、第１認証サーバ６０１と第２認証サーバ７０１の認証レベルを比較する。

【００８８】その結果、第１認証サーバ６０１の認証レベルが第２認証サーバ７０１の認証レベル以上であると判断した場合は、認証トークン検査／更新部６１６において認証トークンを更新し、回答電文作成部６３０において図６（ｃ）に示す回答電文を作成し、第２認証サーバ７０１の回答電文受付部７２８に送信する。

【００８９】図６（ｃ）は、回答電文作成部６３０で作成された回答電文の構造を示す概念模式図である。その後、回答電文受付部７２８は、受け取った新たな認証トークンと、その回答電文に含まれる「信頼されるサーバリスト」とをコンテンツ返却部７１０に渡す。

【００９０】コンテンツ返却部７１０は、第１認証サーバ６０１から受け取った「信頼されるサーバリスト」に基づき、第１認証サーバ６０１から受け取った認証トークンを添付して、ＷＷＷコンテンツ７０３から取得したコンテンツを、認証クライアント端末５０１に送信する。

【００９１】（方法例３）前記装置例に適用する本実施形態例の方法例３につき図６及び図１０を参照して説明する。方法例３は、あるユーザが第１認証サーバ６０１において認証をした後、第１認証サーバ６０１とは異なるサーバである第２認証サーバ７０１に対して認証をする場合に、適用される手法である。

【００９２】そして、方法例３では、第1認証サーバ６０１（認証トークン発行元）の認証レベルが、第2認証サーバ７０１（認証トークン利用先）の認証レベルよりも低いと、仮定する。先ず、前述の方法例１と同様に、ユーザが認証サーバ群（第１認証サーバ６０１及び第２認証サーバ７０１）に対して、初めて認証を行うとする。その後、第１認証サーバ６０１とは異なる第２認証サーバ７０１に対して、認証要求を行うとする。このときの処理手順が図１０に示されている。

【００９３】図１０は、認証トークン発行先の認証サーバの認証レベルが認証トークン利用先の認証サーバの認証レベルよりも低い場合の処理手順を示すフローチャートである。

【００９４】先ず、ユーザは、認証クライアント端末５０１の処理プログラム５０２を起動させて、その処理プログラム５０２に含まれているコンテンツ要求部５０３から第２認証サーバ７０１の処理プログラム７０２の認証開始部７０８に対して、第１認証サーバ６０１で作成された認証トークンを伴なったコンテンツ要求情報を送信することで、コンテンツを要求する。

【００９５】認証開始部７０８は、コンテンツ要求情報を受けた後、その要求内容が認証を必要とするものか判断し、認証が必要である場合は認証処理部７０９を呼び出す。認証処理部７０９は、コンテンツ要求情報に「認証済みの認証トークン」が付属していることを確認し、「信頼するサーバリスト７０７」を参照して、信頼するサーバによって作成された認証トークンであることを確認する。

【００９６】次いで、問合せ電文作成部７２７は、図６（ｂ）に示す問合せ電文を作成し、認証トークン発行元の第１認証サーバ６０１の処理プログラム６０２の問合せ電文受付部６２９に暗号化された電文を送信する。

【００９７】問合せ電文受付部６２９は、第１認証サーバ６０１と第２認証サーバ７０１の認証レベルを比較し、第１認証サーバ６０１の認証レベルが第２認証サーバ７０１の認証レベルよりも低いと判断した場合は、認証トークン検査／更新部６１６において、第１認証サーバ６０１に保管されていた認証トークンを削除し、回答電文作成部６３０において図６（ｄ）に示す回答電文を作成し、第２認証サーバ７０１の回答電文受付部７２８に送信する。

【００９８】図６（ｄ）は、回答電文作成部６３０で作成された回答電文の構造を示す概念模式図である。その後、回答電文受付部７２８は、受け取ったクライアント

情報と有効期限を認証トークン作成部７１１に渡す。

【００９９】認証トークン作成部７１１は、新たに認証トークンを作成し、その認証トークンをコンテンツ返却部７１０に渡す。コンテンツ返却部７１０は、「信頼されるサーバリスト」７０７に基づき、第２認証サーバ７０１で新たに作成された認証トークンを添付して、ＷＷＷコンテンツ７０３から取得したコンテンツを、認証クライアント端末５０１に送信する。

【０１００】

【実施例】最後に、以上の装置例及び方法例で説明したシングルサインオン認証システムを用いて、利用者課金をするビジネスモデルにつき実施例として説明する。図１１は、本発明の一実施例に係る利用者認証システム装置の構成図である。同図において、端末装置１，１，１，…が図１に示す認証クライアント端末５０１に該当し、認証サーバ１２が図１に示す第１認証サーバ６０１及び第２認証サーバ７０１に該当する。

【０１０１】この一実施例に係る利用者認証システム装置δは、ネットワーク２上に、複数の業務サーバ３，３，３，…（業務サーバ群１０）との間のネットワーク接続を可能とするよう設定された代理認証機構５と、複数の業務サーバ３，３，３，…を利用する全ての端末装置１，１，１…（端末装置群１１）の利用者認証を可能とするよう設定されたパスワードデータベース４及び課金データベース９とからなる認証サーバ１２を有して構成される。

【０１０２】ここで、認証サーバ１２における代理認証機構５には、当該認証サーバ１２の手続業務により、全ての端末装置１，１，１，…の各利用者から業務サーバ利用料の集計額を複数の業務サーバ３，３，３，…に代わって代理徴収すると共に、当該複数の業務サーバ３，３，３，…から業務サーバ利用料の徴収代行手数料として認証サーバ使用料を徴収するために、パスワードデータベース４及び課金データベース９を参照することにより、全ての端末装置１，１，１，…の各利用者についての業務サーバ利用料を定期的に集計する処理過程を実行するための処理手段（図示せず）が新たに具備される。

【０１０３】以上の構成において、端末装置群１１における特定の端末装置１が、業務サーバ群１０に含まれる何れかの業務サーバ３を用いてある業務を行った場合、認証サーバ１２は、　パスワードデータベース４及び課金データベース９のデータに基づき、端末装置１の利用者から業務サーバ利用料の代理徴収を行うと共に、　その代理徴収に係る業務サーバ利用料を個々の業務サーバ３，３，３，…へ定期的に支払い、さらに、　個々の業務サーバ３，３，３，…から徴収代行手数料としての認証サーバ使用料を定期的に徴収する（支払いを受ける）。

【０１０４】そして以上により、本来は個々の業務サーバ３，３，３，…にて実施すべき利用者課金業務を、上記認証サーバ使用料を運営資金としながら認証サーバ１２において一括して代行することが可能となり、これに伴い、個々の業務サーバ３，３，３，…にて個別に利用者課金業務を行う必要がなくなって、それら個々の業務サーバ３，３，３，…の運営管理コストの削減を図ることが可能となる。

【０１０５】以上、本発明の実施形態を説明したが、本発明は、必ずしも上記した事項に限定されるものではなく、本発明の目的を達し、下記する効果を奏する範囲において、適宜変更実施可能である。例えば、第１認証サーバ６０１及び第２認証サーバ７０１としては、パーソナル・コンピュータに限らず、ＰＤＡ（Personal Digital Assistants）、携帯電話、パーソナル・ハンディホン・システム（ＰＨＳ）、カーナビゲーションシステム、ゲーム機器等を用いることが可能である。

【０１０６】また、ネットワーク２としては、インターネット及びイントラネットに限らず、エキストラネット、ローカル・エリア・ネットワーク（ＬＡＮ）、公衆電話回線、専用電話回線などを用いたものでもよい。

【０１０７】

【発明の効果】以上説明したように、本発明によれば、ユーザが１回のログインで、複数のサーバにアクセスできるようにするシングルサインオンを提供するシステムにおいて、ユーザの認証状態を複数のサーバで共有する際に、各サーバがユーザの認証状態を分散管理することを可能とするので、認証状態を一元管理する認証状態管理サーバを必要とせずにシングルサインオン・システムを構築することが可能となり、システム構築コスト及び運用管理コストを軽減することが可能となる。

【０１０８】また、複数の認証サーバ間において認証に関する信頼性につき優劣がある場合に、その信頼性の優劣に応じて各サーバでユーザの認証状態を分散管理するので、複数の認証に関する情報から信頼性の高い情報を選択して認証することが可能となり、認証についての信頼性を高めると共に、信頼関係の変化に柔軟に対応した認証状態の共有をすることが可能となる。

【０１０９】また、各サーバ間で共同利用される認証状態を示す情報（認証トークン）につき、サーバの署名の添付及び暗号化を施してネットワーク上を伝送することで、認証についての高度なセキュリティを確保することが可能となる。

【図面の簡単な説明】

【図１】本発明の実施形態である装置例の概念模式図である。

【図２】同上の装置例の動作を示すフローチャートである。

【図３】同上の装置例におけるデータベースの構造を示す図であり、（ａ）は認証データベースの構造を示し、（ｂ）は認証状態管理データベースの構造を示している。

【図４】本発明の実施形態である方法例１において、ユーザが認証サーバ群に初めて認証を求めるときの手順を示すフローチャートである。

【図５】同上の方法例１における認証トークン作成部６１１での処理手順を示すフローチャートである。

【図６】同上の装置例で作成される各種電文の構造を示す概念模式図であり、（ａ）は認証トークンの構造であり、（ｂ）は問合せ電文の構造であり、（ｃ）は回答電文の構造であり、（ｄ）は他の回答電文の構造である。

【図７】同上の方法例１における同一の認証サーバに再度の認証要求が発生した場合の処理手順を示すフローチャートである。

【図８】同上の方法例１における認証トークン検証／更新部６１６の処理手順を示すフローチャートである。

【図９】本発明の実施形態である方法例２において、認証トークン発行元の方が認証トークン利用先よりも認証レベルが高い場合の処理手順を示すフローチャートである。

【図１０】本発明の実施形態である方法例３において、認証トークン発行元よりも認証トークン利用先の方が認証レベルが高い場合の処理手順を示すフローチャートである。

【図１１】本発明の一実施例に係る利用者認証システム装置の構成図である。

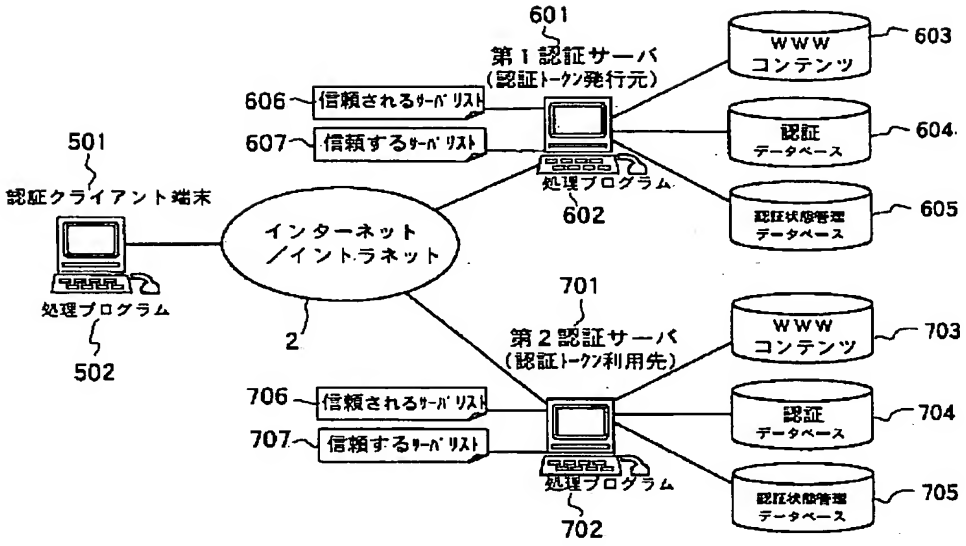
【図１２】従来のシングルサインオン機能を持ったシステム装置の模式概念図である。

【図１３】同上のシステム装置の処理手順を示すフローチャートである。

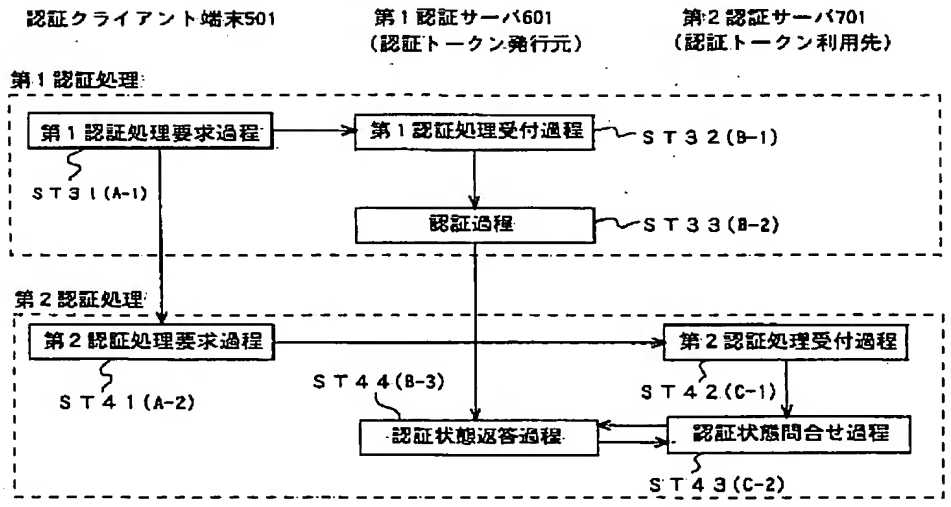
【符号の説明】

δ…一実施例に係る利用者認証システム装置
１…端末装置
２…ネットワーク
３…業務サーバ
４…パスワードデータベース
５…代理認証機構
９…課金データベース
１０…業務サーバ群
１１…端末装置群
１２…認証サーバ
１０１，５０１…認証クライアント端末
１０２，２０２，３０２，４０２，５０２，６０２，７０２…処理プログラム
２０１，３０１，６０１，７０１…認証サーバ
２０３，３０３，６０３，７０３…WWWコンテンツ
４０３，６０４，７０４…認証データベース
４０４，６０５，７０５…認証状態管理データベース
６０６，７０６…信頼されるサーバリスト
６０７，７０７…信頼するサーバリスト
５０３…コンテンツ要求部
５０４…認証処理部
６０８…認証開始部
６０９…認証処理部
６１０…コンテンツ返却部
６１１…認証トークン作成部
６１２…有効期限作成部
６１３…認証ＩＤ作成部
６１４…署名作成部
６１５…共通鍵暗号部
６１６…認証トークン検証／更新部
６１７…認証トークン発行者検証部
６１８…共通鍵復号部
６１９…署名検証部
６２０…認証ＩＤ検証部
６２１…クライアント情報検証部
６２２…有効期限検証部
６２３…有効期限更新部
６２４…認証ＩＤ更新部
６２５…署名作成部
６２６…共通鍵暗号部
６２９…問合せ電文受付部
６３０…回答電文作成部
７０８…認証開始部
７０９…認証処理部
７１０…コンテンツ返却部
７１１…認証トークン作成部
７２７…問合せ電文作成部
７２８…回答電文受付部

【図１】


601
第１認証サーバ
(認証トークン発行元)
WWW
コンテンツ
603
606
信頼されるサーバリスト
607
信頼するサーバリスト
認証
データベース
604
501
認証クライアント端末
処理プログラム
602
認証状態管理
データベース
605
インターネット
／イントラネット
701
処理プログラム
502
2
第２認証サーバ
(認証トークン利用先)
WWW
コンテンツ
703
706
信頼されるサーバリスト
707
信頼するサーバリスト
認証
データベース
704
処理プログラム
認証状態管理
データベース
705
702

【図２】


認証クライアント端末501
第１認証サーバ601
(認証トークン発行元)
第２認証サーバ701
(認証トークン利用先)
第１認証処理
第１認証処理要求過程
第１認証処理受付過程
ＳＴ３２(B-1)
ＳＴ３１(A-1)
認証過程
ＳＴ３３(B-2)
第２認証処理
第２認証処理要求過程
第２認証処理受付過程
ＳＴ４４(B-3)
ＳＴ４２(C-1)
ＳＴ４１(A-2)
認証状態返答過程
認証状態問合せ過程
ＳＴ４３(C-2)

【図３】

認証データベース

カラム名	説明
ユーザＩＤ	認証対象のユーザＩＤ
パスワード	認証対象のユーザのパスワード
⋮	その他、ユーザを特定する情報

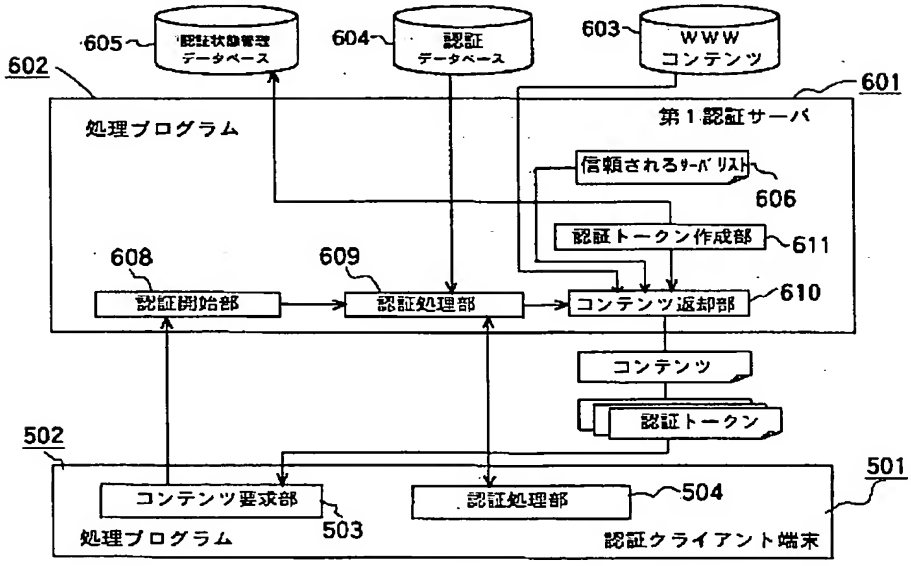
（ａ）

認証状態管理データベース

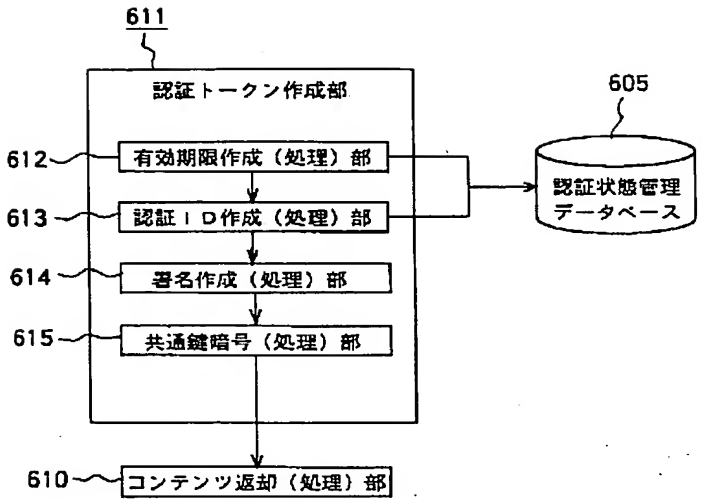
カラム名	説明
ユーザＩＤ	認証済みユーザＩＤ
認証ＩＤ	アクセスごとに変更する一時的なＩＤ
クライアントアドレス	クライアントアドレス
有効期限	認証状態の有効期間
⋮	その他、クライアントを特定する情報

（ｂ）

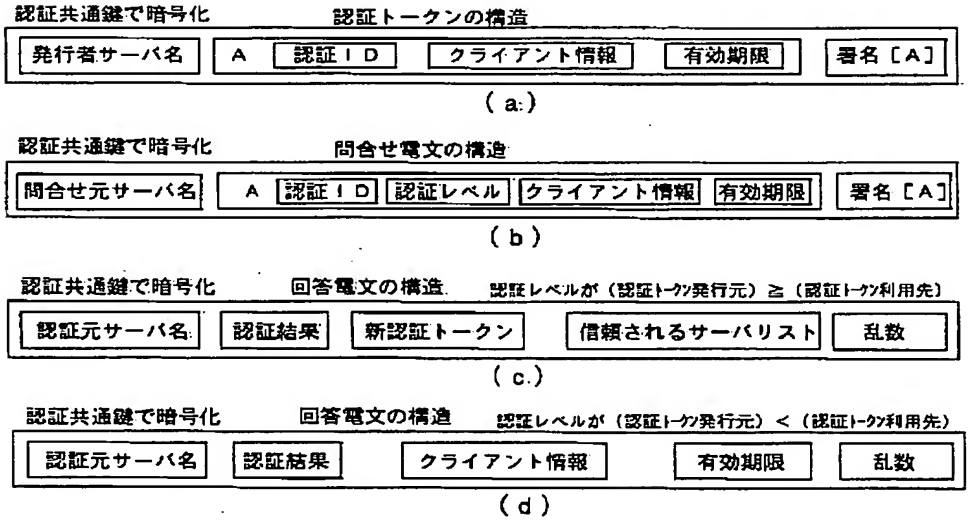
【図４】



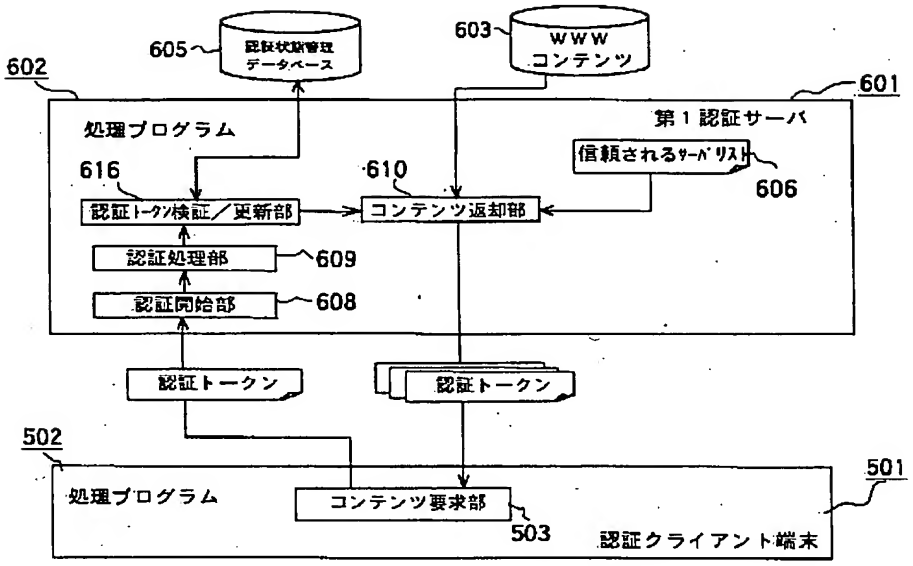
【図５】


611
認証トークン作成部
605
612
有効期限作成（処理）部
613
認証ＩＤ作成（処理）部
614
署名作成（処理）部
615
共通鍵暗号（処理）部
認証状態管理
データベース
610
コンテンツ返却（処理）部

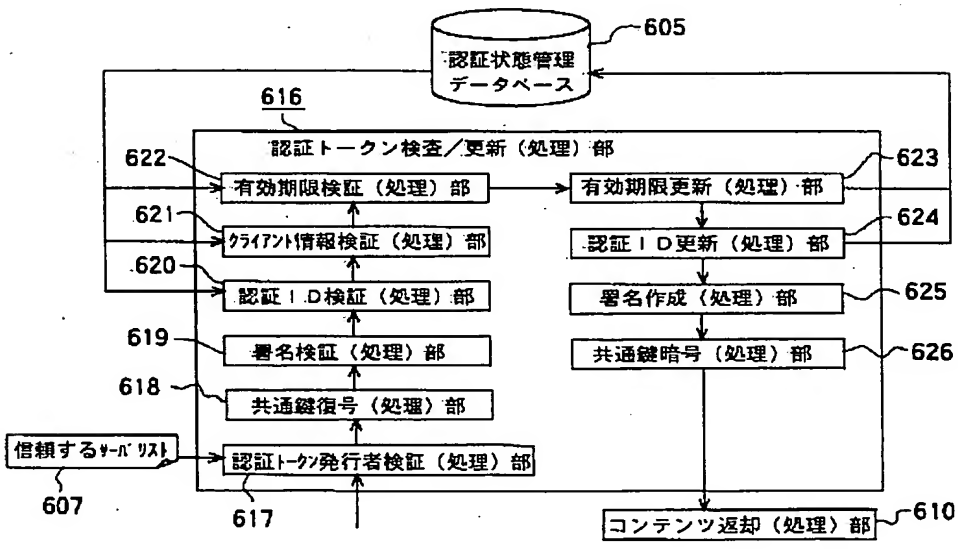
【図６】


認証共通鍵で暗号化
認証トークンの構造
発行者サーバ名
A
認証ＩＤ
クライアント情報
有効期限
署名［A］
(a)
認証共通鍵で暗号化
問合せ電文の構造
問合せ元サーバ名
A
認証ＩＤ
認証レベル
クライアント情報
有効期限
署名［A］
(b)
認証共通鍵で暗号化
回答電文の構造
認証レベルが（認証トークン発行元）≧（認証トークン利用先）
認証元サーバ名
認証結果
新認証トークン
信頼されるサーバリスト
乱数
(c)
認証共通鍵で暗号化
回答電文の構造
認証レベルが（認証トークン発行元）＜（認証トークン利用先）
認証元サーバ名
認証結果
クライアント情報
有効期限
乱数
(d)

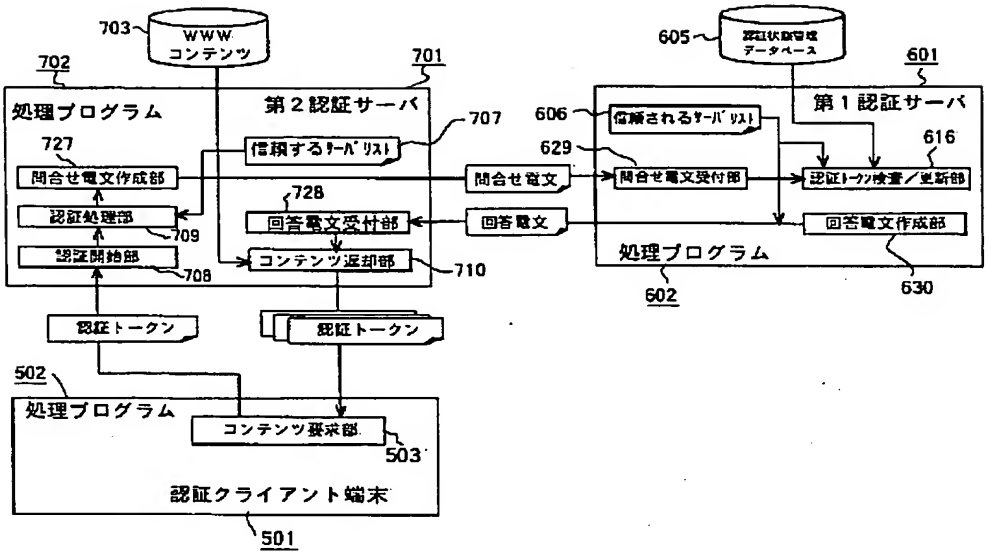
【図７】


605
認証状態管理
データベース
603
WWW
コンテンツ
602
601
処理プログラム
第１認証サーバ
信頼されるｻｰﾊﾞﾘｽﾄ
606
616
610
認証ﾄｰｸﾝ検証／更新部
コンテンツ返却部
認証処理部
609
認証開始部
608
認証トークン
認証トークン
502
501
処理プログラム
コンテンツ要求部
503
認証クライアント端末

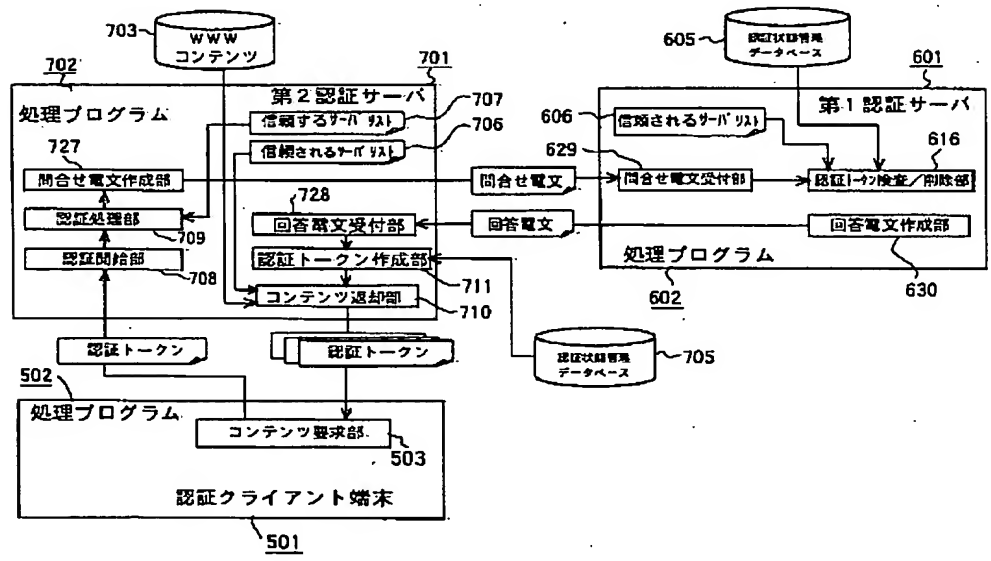
【図８】


605
認証状態管理
データベース
616
認証トークン検査／更新（処理）部
622
有効期限検証（処理）部
623
有効期限更新（処理）部
621
ｸﾗｲｱﾝﾄ情報検証（処理）部
624
認証ＩＤ更新（処理）部
620
認証ＩＤ検証（処理）部
625
署名作成（処理）部
619
署名検証（処理）部
626
共通鍵暗号（処理）部
618
共通鍵復号（処理）部
信頼するｻｰﾊﾞﾘｽﾄ
607
認証ﾄｰｸﾝ発行者検証（処理）部
617
コンテンツ返却（処理）部
610

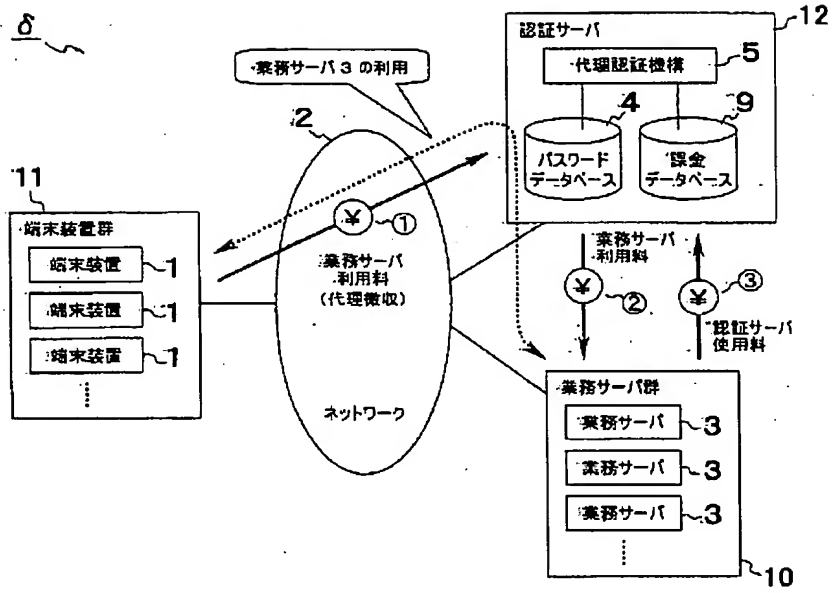
【図９】


703
WWW
コンテンツ
702
701
処理プログラム
第２認証サーバ
707
信頼するサーバリスト
727
問合せ電文作成部
認証処理部
709
認証開始部
708
728
回答電文受付部
コンテンツ返却部
710
605
認証状態管理
データベース
601
第１認証サーバ
606
信頼されるサーバリスト
629
問合せ電文受付部
616
認証トークン検査／更新部
問合せ電文
回答電文
回答電文作成部
処理プログラム
602
630
認証トークン
認証トークン
502
処理プログラム
コンテンツ要求部
503
認証クライアント端末
501

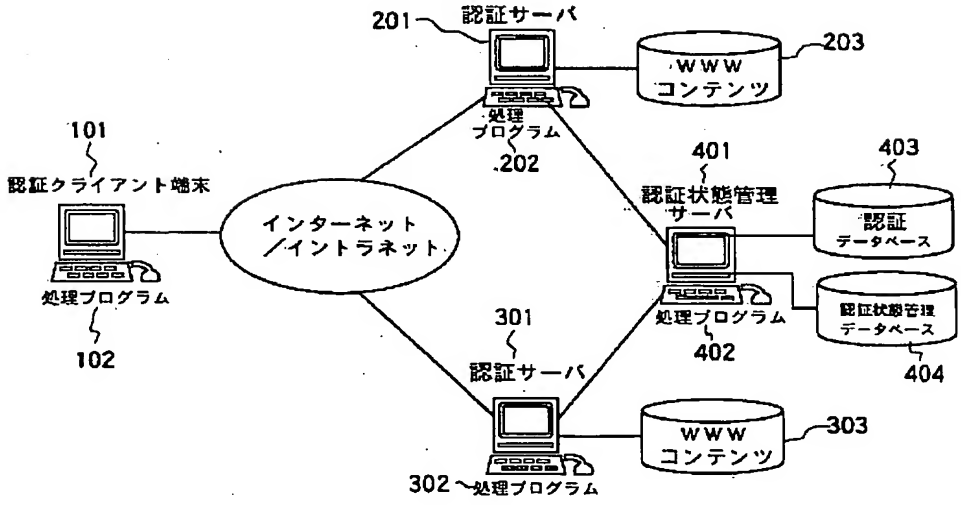
【図１０】


703
WWW
コンテンツ
702
701
処理プログラム
第２認証サーバ
707
信頼するサーバリスト
706
信頼されるサーバリスト
727
問合せ電文作成部
認証処理部
709
認証開始部
708
728
回答電文受付部
認証トークン作成部
711
コンテンツ返却部
710
605
認証状態管理
データベース
601
第１認証サーバ
606
信頼されるサーバリスト
629
問合せ電文受付部
616
認証トークン検査／削除部
問合せ電文
回答電文
回答電文作成部
処理プログラム
602
630
705
認証トークン
認証トークン
502
処理プログラム
コンテンツ要求部
503
認証クライアント端末
501

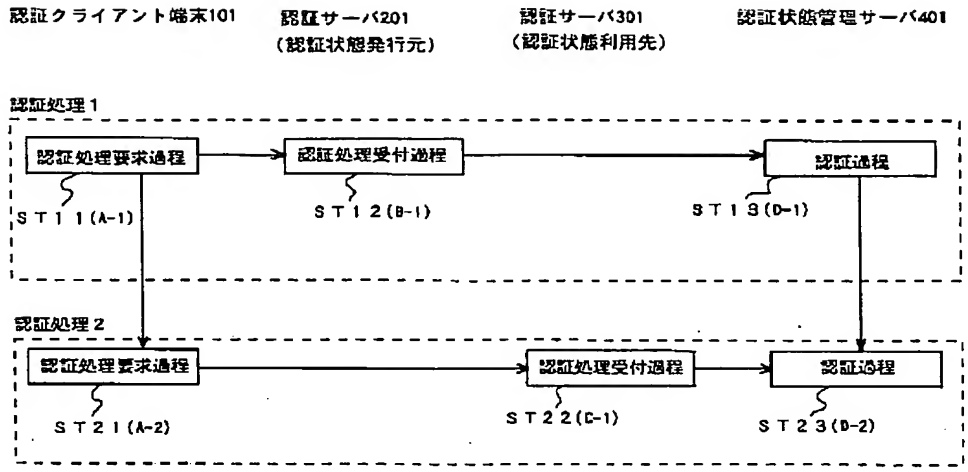
【図１１】


δ
業務サーバ３の利用
2
認証サーバ
12
代理認証機構
5
4
9
パスワード
データベース
課金
データベース
11
端末装置群
端末装置
1
端末装置
1
端末装置
1
¥
①
業務サーバ
利用料
（代理徴収）
ネットワーク
業務サーバ
利用料
¥
②
¥
③
認証サーバ
使用料
業務サーバ群
業務サーバ
3
業務サーバ
3
業務サーバ
3
10

【図１２】


201
認証サーバ
WWW
コンテンツ
203
処理
プログラム
202
101
認証クライアント端末
インターネット
／イントラネット
401
認証状態管理
サーバ
403
認証
データベース
処理プログラム
402
認証状態管理
データベース
404
処理プログラム
102
301
認証サーバ
WWW
コンテンツ
303
302
処理プログラム

【図１３】



フロントページの続き

Ｆターム(参考)　5B085 AE00 AE02 BC01
5J104 AA08 KA01 KA02 MA03 NA05
PA07